

REMARKS

Claims 48, 49, and 59-61 have been previously cancelled. New claims 62-77 have been added via the present amendment. By this amendment claims 1-3, 5-47, 50-58 and 62-77 are in the application. Reconsideration of the patentability of the claims is respectfully requested view of the following remarks.

Claim 1 as now amended is directed to a data transfer apparatus for secure transfer from a digital data source to a digital data receiver of a plurality of data blocks each data block comprising plural frames of a digital video image. The apparatus comprises in combination various elements that include an encryption key generator for providing encryption keys wherein a respective encryption key is assigned to each data block of the plurality of data blocks and a block synchronization index is provided indicating a correspondence between the encryption key and the data block. An encryption engine for each data block, produces an encrypted data block using the encryption key from the encryption key generator. A data transmission channel is provided for delivering the encrypted data block from the encryption engine to the digital data receiver. A key transmission channel is provided for delivering the encryption key from the encryption key generator to the digital data receiver. A block synchronization data channel is provided for delivering the block synchronization index from the encryption key generator to the digital data receiver. A memory stores the encryption keys at the digital data receiver; and the digital data receiver includes a decryption engine that is responsive to the synchronization index for mapping each key in a memory to a respective encrypted data block for use in decryption of the respective data block.

As amended claim 1 now calls for a block synchronization data channel for delivering a block synchronization index from the encryption key generator to the digital data receiver. A memory stores the encryption keys at the digital data receiver and the digital data receiver includes a decryption engine that is responsive to the synchronization index for mapping each key in a memory to a respective encrypted data block for use in decryption of the respective data blocks. The Examiner has cited Warren as disclosing that each data block contains the encryption key for the frame contained in the next data block. There is no specific index identified by Warren nor is there any disclosure that such a synchronization index is used to map each key in a memory to a respective

encrypted data block. As disclosed in the specification this allows for the variability of image block sizes which is not possible in the specific embodiments of Warren cited by the Examiner wherein each key has a fixed position relative its corresponding frame. The Examiner is reminded that anticipation requires that the reference show all the features of the claimed invention. It is further submitted that claim 1 and claims dependent therefrom are not obvious in view of Warren either alone or taken in view of any of the other references since the prior art does not disclose the feature of the use of the index to provide this map in accordance with the combination of elements of claim 1.

Dependent claims 11 and 14 are dependent upon claim 1 and further delimit this claim with the feature regarding the use of a smartcard for the block synchronization data channel and for the key transmission channel respectively. The Examiner has cited the combination of Warren in view of Handleman as rendering obvious this combination. The Examiner acknowledges that Warren does not disclose using smart cards in the copy management system and notes that the secondary reference, Handleman, discloses a data access system wherein video data is accessed using a smartcard that communicates seeds, keys and access control algorithms with the video decoder. However, a careful reading of the paragraph of Handleman noted by the Examiner indicates that it is the video data stored in the IC card that access is provided to and that there is no disclosure of the use of the block synchronization data channel that utilizes a smartcard. Nor, is there disclosure of a key transmission channel that utilizes a smartcard. For this reason it is submitted that claims 11 and 14 are patentable over the combination of Warren taken with Handleman.

Dependent claims 12 and 18 are dependent upon claim 1 and stand rejected as being obvious in view of Warren. Regarding claim 12 the Examiner opines that it would be obvious to encrypt the synchronization index even though no specific index is disclosed by Warren, the Examiner using the possible teaching in Warren of relative position to be the equivalent of an index. However no specific index is disclosed in Warren and therefore it is not seen how such could render obvious a claimed combination reciting encryption of such an index. Furthermore, it is additionally not seen how lack of specific disclosure of a block synchronization index in Warren could render obvious a claimed combination calling for such a synchronization index to be computed using a pseudo-random

numbered generator. For this reason it is submitted that claims 12 and 18 are not obvious in view of Warren or any combination of references cited by the Examiner.

Dependent claim 19 is rejected under 35 USC 103 as being unpatentable over Warren in view of Schneier. Claim 19 is a dependent claim of claim 18 and further delimits this claim by reciting that the pseudo-random numbered generator is a linear feedback shift register. As noted above, dependent claim 18 adds the feature to claim 1 that the block synchronization index is computed using a pseudo-random numbered generator. In the specific disclosure of Warren referred to by the Examiner a block synchronization index is not computed using any pseudo-random number generator and the Examiner acknowledges that Warren fails to even teach that such an index is generated randomly. Despite this lack of teaching by Warren and particularly the lack of any suggestion in Warren of any specific index that is generated it is not seen how one of ordinary skill in the art would be directed to consider Schneier for the general teaching that pseudo-random sequences can be generated using linear feedback shift registers when there is no indication in Warren of providing for a randomly generated index in the first place. It is clear that this combination of references can only have been suggested through resort to an advance reading of applicant's specification and thus constitutes an improper hindsight reconstruction of the prior art. It is thus respectfully submitted that claim 19 is patentable over the prior art.

Independent claim 20 is directed to a method for secure transfer of a data stream from a digital data source to a digital data receiver. The method comprises the steps of partitioning the data stream into a plurality of successive data blocks, wherein the size of each successive data block is variable, based on an average size and based on a randomly generated offset. For each successive data block, an encryption key is generated and each successive data block uses the encryption key to provide an encrypted data block. A synchronization index associates the encrypted data block with the encryption key.

The Examiner has rejected claim 20 as being unpatentable over Warren in view of Rump under 35 USC 103. The Examiner notes correctly that Warren fails to teach or disclose that different sized data blocks are provided and identified by an offset value. The Examiner cites Rump for the proposition that

Rump discloses a system for encryption and decryption of multimedia data wherein each block contains a block size index "which meets the limitation of the size of said single data block is further conditioned by an offset value, the size of the successive data block is based on an average size and based on a randomly generated offset." However, the Examiner is using language from applicant's claim rather than from any disclosure of Rump. Rump is merely disclosing that a block size index consists of two sub-entrees; i.e. "step" and "amount" and this is shown in Fig. 3 of Rump. Step indicates the total amount of multimedia data which are assigned to a specific definition data block. Amount indicates the amount of ciphered data in this block. There is no disclosure in Rump of the claimed feature of providing data blocks that are variable based on an average size and based on a randomly generated offset. For this reason it is submitted that claim 20 is patentable over the cited prior art.

Claims 21-25 and 27 are dependent either directly or indirectly from claim 20 and are also submitted to be patentable for the reasons provided above.

Claim 26 stands rejected as being unpatentable over Warren in view of Dahan. The Examiner will note that claim 26 is a dependent claim of claim 20 and therefore includes the subject matter of this claim. Claim 26 adds the feature of the step of transmitting the encrypted data blocks to the receiver side in a non-sequential order. The Examiner cites Dahan as disclosing that data is written from an optical disk in a non-sequential order. However there is no disclosure in this combination of the subject matter described above with regard to claim 20 from which claim 26 depends. The Examiner has acknowledged that Warren fails to disclose this feature and applicant has shown that not even the combination of Warren with Rump renders obvious the subject matter of claim 20. As there is no indication by the Examiner that Dahan even suggests this feature it is submitted that claim 26 is patentable over the prior art.

Claim 3 is a dependent claim of claim 1 and stands rejected as being unpatentable over the combination Warren taken with Rump. Claim 3 is directed to the feature that the size of the data block is further conditioned by an offset value. This feature allows for the provision of different sizes of data blocks to be defined in a relatively compact manner. The Examiner acknowledges that Warren does not disclose different size data blocks being identified by an offset

value. While Rump discloses definition data that identifies size of the data block there is no indication that such is identified by an offset value. Indeed, it appears the Examiner has had to resort to the applicant's claim language to support what Rump does not disclose. For this reason it is submitted that Claim 3 is patentable over the prior art.

Claim 28 has been amended to recite a method for the secure transfer of a digital motion image data stream from a digital data source to a digital data receiver wherein the encryption keys at the digital data receiver are stored in a memory and the digital data receiver includes a decryption engine that is responsive to the synchronization index. Claim 28 further recites that the decryption engine maps each key in a memory to a respective encrypted data block for use in decryption of the respective data block. It is submitted that Warren does not disclose any specific synchronization index and certainly does not disclose the use of any memory to support respective keys in a memory that are mapped by a synchronization index. It is submitted therefore that claim 28 is patentable over Warren either taken alone or in view of the other prior art of record. For similar reasons it is submitted that dependent claims 30, 31-35 which are dependent upon claim 28 are also patentable over Warren either taken alone or in view of the other prior art of record.

Claim 29 is a dependent claim of claim 28 and further delimits this claim with the step of generating an offset value that is used to establish a starting frame for each digital motion image data block. The Examiner has rejected this claim as being unpatentable over Warren in view of Rump under 35 USC 103. The Examiner acknowledges that Warren does not disclose different size data blocks being identified by an offset value. While Rump discloses definition data that identifies size of the data block there is no indication that such is identified by an offset value. Indeed, as stated above it appears the Examiner has had to resort to the applicant's claim language to support what Rump does not disclose. For this reason it is submitted that Claim 29 is patentable over the prior art.

Claim 36 is an independent claim that is directed to a method for mapping a plurality of encryption keys to a corresponding plurality of encrypted data blocks of a digital motion image, the method includes the steps of providing the plurality of encryption keys separately from said encrypted data blocks and

storing the encryption keys in a memory at a digital data receiver. The method is further characterized by providing an identifier that correlates a mapping algorithm to the plurality of encryption keys. A decryption engine is operated so that it is responsive to the identifier and the mapping algorithm to generate each key for use in decryption of the respective data block. It is respectfully submitted that this claim is also patentable over Warren either taken alone or in combination with any of the other references of record. While it is acknowledged that Warren discloses the synchronization of an encryption key for the frame there is no storing of the encryption keys in a memory at the digital data receiver and no providing of an identifier that correlates a mapping algorithm to the plurality of encryption keys. It is submitted therefore that claim 36 as now amended is patentable over the prior art of record. It is further submitted that dependent claims 38-41, 43 and 44 which depend either directly or indirectly from claim 36 are also patentable over the prior art of record.

Claim 37 is a dependent claim of claim 36 and adds the feature that the plurality of encryption keys are interleaved in a nonsequential order. The Examiner has rejected this claim as being unpatentable over the combination of Warren taken with Dahan. With the amendment of claim 36 it is submitted that applicants have overcome any issue of unpatentability with regard to claim 37. Furthermore, as noted above the Examiner cites Dahan as disclosing that data is written from an optical disk in a non-sequential order. However, the Examiner is urged to consider the claim as a whole and to consider what is specifically being claimed in claim 37. There is no suggestion in either Warren or in Dahan or in their combination of storing the plurality of encryption keys as being interleaved in a nonsequential order. For this reason it is respectfully submitted that claim 37 is patentable over the prior art of record.

Claims 42, 45 and 46 are dependent claims which depend directly or indirectly from claim 39 which in turn is a dependent claim of independent claim 36. As noted above claim 36 is amended to define a method that includes the steps of providing the plurality of encryption keys separately from the encrypted data blocks and storing the encryption keys in a memory at a digital data receiver. The method is further characterized by providing an identifier that correlates a mapping algorithm to the plurality of encryption keys. A decryption engine is operated so that it is responsive to the identifier and the mapping

algorithm to generate each key for use in decryption of the respective data block. Chaum is cited by the Examiner as providing disclosure of a copy protection system that utilizes two video parts in combination at a projector to view the film. However Chaum is not concerned with encryption nor is there any suggestion made by the Examiner as to why one of ordinary skill in the art would consider this reference other than for the fact that a projector is a known way for projecting a film image. Warren still fails either taken alone or in combination with Chaum or the other prior art of record to render obvious the subject matter of claims 36 and of claim 39 from which claims 42, 45 and 46 depend. For this reason it is respectfully submitted that claims 42, 45 and 46 are patentable over Warren taken with Chaum or any other prior art of record.

Claim 47 is an independent claim directed to a method of decrypting encrypted digital motion image data blocks of a motion picture. As presently amended this method comprises the steps of providing digital motion image data of a digital motion picture as digital motion image data blocks at least some of which digital motion image data blocks are of different sizes to provide at least some variability in terms of numbers of frames of said motion picture in said image data blocks; and in response to an index providing information identifying a first frame of each digital motion image data block generating a corresponding key from a plurality of encryption keys for use in decrypting a respective digital motion image data block wherein the at least some digital motion image data blocks each represents plural frames of the motion picture. Claim 47 has been rejected as being unpatentable over Warren in view of Rump. The present amendment of this claim has the additional feature of providing at least some variability in terms of numbers of frames of the motion picture in the image data blocks and in response to an index providing information identifying a first frame of each digital motion image data block generating a corresponding key from a plurality of encryption keys for use in decrypting the respective digital motion image data block. The Examiner has acknowledged that Warren does not disclose having different size data blocks. The Examiner has cited Rump as disclosing a system for encryption and decryption of multimedia data wherein each block contains a block size index. However, it is respectfully submitted that the combination of claim 47 in particular the feature of an index providing information identifying a first frame of each digital motion image data block is

not taught or suggested by the combination of Warren taken in view Rump. For this reason it is respectfully submitted that claim 47 is patentable over the combination of Warren taken with Rump or any other prior art of record. Furthermore, it is respectfully submitted that claim 58 which depends from claim 47 is patentable over Warren either taken alone or in combination with any other prior art cited by the Examiner.

Claim 57 is a dependent claim of claim 47 and adds the feature that the block boundaries are determined by computation of random offsets. The Examiner acknowledges that Warren does not disclose different size data blocks identified by an offset value. While Rump discloses encryption and decryption of multimedia data wherein there is a block size index, there is no disclosure in this reference that the block boundaries of the movie image are determined by computation of random offsets. For this reason it is submitted that claim 57 is patentable over the combination of Warren taken with Rump.

Claim 50 is a dependent claim of claim 47 and adds the feature that the decryption of the encrypted data blocks is made in a digital motion image projector. The Examiner has rejected this claim as being unpatentable over Warren in view of Chaum. However, claim 50 incorporates the subject matter of claim 47 from which it depends and it is submitted that Chaum would not suggest itself to the routineer having the Warren reference before him/her. Chaum merely discloses the use of two projectors for obscuring a part of a movie. There is no disclosure in Chaum regarding the use of encryption keys in accordance with the combination claimed in independent claim 47 as now amended. Neither Warren nor Chaum teach of a method of providing at least some variability in terms of numbers of frames of a motion picture in the image data blocks and in response to an index providing information identifying a first frame of each digital motion image data block generating a corresponding key from a plurality of encryption keys for use in decrypting the respective digital motion image data block. It is respectfully submitted therefore that claim 47 is patentable over the combination of Warren taken with Chaum or with any other prior art of record.

Claim 52 is an independent claim directed to a method of decrypting encrypted digital motion image data blocks of a motion picture wherein digital motion image data of a digital motion picture is provided as digital motion image data blocks. The digital motion image data blocks are

compressed using an MPEG type of compression to form intra-coded stand alone frames and dependent P and B frames, and the intra-coded and P and B frames are encrypted. A corresponding key from a plurality of encryption keys is generated for use in decrypting a digital motion image data block that is encrypted. The Examiner indicates that Warren discloses the use of MPEG type of compression, however there is no indication in this reference regarding the compression of the types of frames set forth in claim 52. The Examiner is reminded that for a reference to anticipate there must be a showing of all features of the claimed subject matter within the single reference itself. Since it is acknowledged in applicant's specification that it is known that encryption of only one of the frame components, the I- frame, of an MPEG compression is known but not the dependent frames it is incumbent of the Examiner to demonstrate through teachings in the prior art that the subject matter of claim 52 is unpatentable. It is respectfully submitted that this has not been done. As noted in applicant's specification, see page 6, the method of the prior art may be problematic in that frame boundaries in the cipher text datastream may remain obvious which is disadvantages from a data security perspective. For this reason claim 52 should be patentable over the prior art of record.

Claim 53 is an independent claim directed to a method of decrypting encrypted digital motion image data blocks of a motion picture. In accordance with the method, digital motion image data of a digital motion picture is provided as digital motion image data blocks, wherein a digital motion image data frame comprises plural color components and only data of one of the color components is encrypted. A corresponding key from a plurality of encryption keys is generated for use in decrypting a digital motion image data block that is encrypted. The Examiner has recognized that Warren alone does not anticipate or render obvious this claim. Chaum is noted by the Examiner for a general teaching of protection of a frame through manipulation of a particular color within the frame. However, Chaum is not directed to encryption or decryption of digital data but merely preventing the video capture of a projected image of such a motion picture. It can be hardly said that the disclosure of Chaum would be considered of any use to the routineer with regard to the problem applicant has solved. Once again it is respectfully submitted that the Examiner has improperly used a hindsight reconstruction of the prior art without identifying what would

motivate the routineer to consider Chaum as being pertinent to the subject matter of claim 53. Similarly, claim 54 is a dependent claim of claim 53 and also should be patentable over the combination of Warren taken with Chaum.

Claim 55 is a dependent claim of claim 47 and is also submitted to be patentable over the combination of Warren taken with Chaum. Claim 47 as noted above is directed to a method wherein a motion picture is provided as digital motion image data blocks at least some of which digital motion image data blocks are of different sizes in terms of number of frames of the motion picture. A corresponding key is generated from a plurality of encryption keys for use in decryption of a respective digital motion image data block wherein the digital motion image data blocks each represent plural frames of the motion picture. Claim 55 is further distinguished in that the digital motion image data frame comprises plural color components and the data of the color components are encrypted. As noted above and acknowledged by the Examiner, Warren does not disclose that the video signal is encrypted based on color data. While Chaum discloses that protection can be provided for videotaping of a projected color image by manipulating image data in a frame there is no suggestion of encryption in accordance with the subject matter of claim 55. The Examiner has failed to show any reason why one of ordinary skill in the art would consider Chaum of any use in the process of Warren. Warren is involved with encryption of the video image while Chaum is involved with the theft of a projected image. It is submitted therefore that claim 55 should be patentable over the prior art. Claim 56 is a dependent claim 55 and should be patentable for the same reasons provided.

For many of the reasons provided above it is respectfully submitted that newly submitted claims 62-77 are also patentable over the prior art.

It is believed that the application is now in condition for allowance prompt notice of which is urgently solicited. However, if the Examiner is of the opinion that additional modifications to the claims are necessary to place the application in condition for allowance, he is invited to contact applicant's attorney at the number listed below for a telephone interview for an Examiner's amendment.

Respectfully submitted,



Attorney for Applicant(s)
Registration No. 29,134

Nelson A. Blish/tmp
Rochester, NY 14650
Telephone: 585-588-2720
Facsimile: 585-477-4646

If the Examiner is unable to reach the Applicant(s) Attorney at the telephone number provided, the Examiner is requested to communicate with Eastman Kodak Company Patent Operations at (585) 477-4656.